Issue 390 | November 2019

EXTRACT

# Banking Automation BULLETIN


**Banks reduce their footprint as branches get smarter**

Can the global cards market keep growing at its current rate?

UnionPay retains largest share of global card expenditure

Information sharing still seen as key to crime prevention

Cash and ATM usage continue to decline in the UK

**Country profile: Singapore**

rbr

Published by RBR since 1979

www.rbrlondon.com/bulletin

GMV PERSPECTIVE

# And now Windows 10... Are you serious?

*By Angel Fco. Zato del Corral, Technical Leader, GMV*

*Angel Fco. Zato del Corral*
GMV

Though we still haven't recovered from the migration to Windows 7, we have to embark on a new one now. The migration to Windows 10, which a few brave souls already have under way, seems even more complicated than the earlier one. The list of changes and new features incorporated lets us glimpse the associated impact, from the most visible and best-known changes like the hardware updates required for the oldest ATMs, to other changes, which, though less well known, have a profound impact on all the software of the system.

Even though the list of changes is long, the list of new features is too, and many of the latter entail significant improvements in the stability, robustness and security of the system. Unquestionably, this list of novelties easily justifies the effort of migration and sweetens the bitter pill of two migrations almost on top of each other.

**The list of new Windows 10 features is long, and these entail significant improvements in the stability, robustness and security of the system**

Below, we will try to summarise and answer questions on the most important changes and novelties brought by Windows 10, from the software perspective and, more specifically, in the logical security of the system.

Many of the features of Windows 10 have to do with technologies which have been getting incorporated into the PC world over the last decade, but which for one reason or another have lain dormant for years. UEFI, GPT, Secure Boot and TPM are probably some of the terms that have arrived with Windows 10, and about which there is a lot of confusion with respect to their utility, necessity and desirability.

## UEFI: the firmware that supersedes BIOS

This acronym crops up every time people speak of Windows 10, as though the two were twins. UEFI is the acronym for Unified Extensible Firmware Interface: in other words, it is an interface for communication between the firmware installed on the PC motherboard and the operating system. In reality, UEFI is the specification setting out how this communication takes place. A useful simplification, although not completely precise, is to think of UEFI as the type of firmware which replaces the traditional BIOS (Basic Input Output System) firmware, present in PCs. UEFI firmware has a BIOS emulation mode, known as CSM (Compatibility Support Module), which makes the computer's UEFI firmware behave exactly as BIOS firmware would, which means we may find it present already on machines running Windows 7.

What does UEFI really deliver in contrast to BIOS? We could list a number of improvements, from a prettier and more user-friendly graphical user interface, to the possibility of adding third-party components to extend the capabilities of the firmware. Thinking of ATM networks, the most interesting improvements are: The removal of the constraints on the maximum hard disk size (2.2 TB) and number of primary partitions (four) imposed by the MBR standard; and the incorporation of the technology Secure Boot.

Apart from improvements, does installing Windows 10 make having UEFI firmware mandatory? The answer is simply, no. Microsoft does not specify that having UEFI firmware is necessary to install Windows 10. In fact, Windows 10 can be installed and will behave in exactly the same way on an ATM with BIOS firmware or UEFI firmware, whether or not the latter is configured in BIOS compatibility mode. However, it must be borne in mind that certain features can only be enabled with UEFI firmware, so that this option is the one recommended by Microsoft to obtain the greatest performance. For instance, to enable Secure Boot, it is indispensable to have UEFI firmware with the BIOS compatibility mode deactivated.

## GPT: the new hard disk partitioning standard

Another acronym we mentioned earlier is GPT (GUID Partition Table). This is a new standard for partitioning (the creation of logical divisions) for hard disks, based on GUIDs. A GUID is a unique global identifier referencing the partitions defined on the disk. Just as we consider UEFI as the replacement for BIOS, GPT supersedes the well-known MBR (Master Boot Record) scheme which has dominated the market for so many years.

So, is GPT partitioning necessary for Windows 10? Again, the answer is no. Windows 10 can be installed on a hard disk partitioned using the MBR layout. But if I would like my installation of Windows 10 to let me harness the advantages of the UEFI firmware, it does become necessary to use a GPT. This is because the UEFI specification requires the presence of a partition table of this type, in which there must exist one special partition known as the EFI System Partition (ESP), which will be utilised by the firmware.

### TPM: the anti-sabotage cryptographic chip

The TPM (Trusted Platform Module) is a secure cryptographic processor typically implemented in dedicated hardware installed on the PC motherboard. The TPM has been present in the majority of ATMs since 2012. This processor offers various features, among the most important of which are the capability to generate and store cryptographic keys securely, and the creation of unforgeable identifiers derived from the configuration of the machine's hardware and software. This latter capability is the one used to validate the integrity of the platform, which is the PC in the case of ATMs, and makes it possible to determine whether it was booted using the proper succession of trusted software components without the intervention of any malicious or tampered-with elements.

Certain Windows 10 security features such as Measured Boot, Bitlocker and Device Health Attestation can only be activated if there is a TPM present. From the security point of view, the importance this specialised device has acquired is such that in July 2018, Microsoft decided to make it a mandatory requirement for the installation of Windows 10 on new machines. Microsoft established at that moment not only that the TPM must be present in the device, but that it must be enabled and available to the operating system by default. Only for IoT Core versions of Windows 10 did Microsoft make the presence of the TPM optional.

But in that case, do I need ATMs to have a TPM? If the aim is to attain a high level of security, a requisite somewhere between highly desirable and indispensable when we speak of cash machines, the answer is yes, definitely.

### Secure Boot: the interesting and unfairly neglected feature of UEFI firmware

The last of the technologies we will cover is really an optional characteristic provided by UEFI firmware. Secure Boot is not a component of Windows 10 but a security feature defined in the UEFI specification, which is maintained by the UEFI Forum.

The objective of Secure Boot is very simple: to guarantee that the OS bootloader has been signed by a trusted entity. To this end, the firmware holds an internal store of trusted digital certificates which are loaded during its installation onto the device. This mechanism prevents the running of unsigned bootloaders or those no longer trusted, therefore preventing the execution of a bootkit (malware designed to be run before the OS is loaded).

Once Secure Boot has validated the OS bootloader and has allowed it to take control, responsibility for continuing the validation of the components involved in the boot lies with the operating system itself from that point. The array of Windows services responsible for carrying out this task is given the name of Trusted Boot. Therefore, Trusted Boot comes after Secure Boot, and the joint action of the two is what enables the entire boot sequence to be validated.

Do I need to have a TPM to enable Secure Boot? No. Secure Boot is a characteristic of the UEFI firmware, which already contains all the resources necessary to implement it. Nonetheless, using the TPM complements Secure Boot perfectly, yielding a completely secure boot environment. In fact, the TPM is responsible for measuring metrics of the firmware to guarantee it has not been tampered with, thus constituting an additional protection.

The advent of Windows 10 for ATMs not only brings with it security improvements incorporated into the operating system itself, but also encourages the use of other platform features which enhance the overall level of security. Just like the links in a chain, the different measures the technologies described here put at our disposal are designed to work as a team, given that the absence or deactivation of any of them weakens overall security considerably.

All the features and novelties covered here, together with the others incorporated into Windows 10, are in themselves sufficient grounds to undertake the migration, but they also invite us to do it properly, evaluating all the possible options and setting aside the haste prompted by the End Of Life threat for Windows 7. As we said at the time in relation to Windows XP, ATM networks protected by whitelisting and encrypted hard disk solutions are going to maintain an identical level of protection before and after End Of Life; as was the case then, it's not the end of the world now. ■

**The different measures are designed to work as a team, given that the absence or deactivation of any of them weakens overall security considerably**

**All the features and novelties incorporated into Windows 10 are in themselves sufficient grounds to undertake the migration**